



DEPARTMENT OF THE NAVY

NAVAL SCHOOL OF HEALTH SCIENCES
BETHESDA, MARYLAND 20889-5612

IN REPLY REFER TO:

NSHSBETHINST 5230.3A

21 OCT -6 1999

NSHS BETHESDA INSTRUCTION 5230.3A

From: Commanding Officer

Subj: INFORMATION MANAGEMENT PLAN

Ref: (a) NSHSBETHINST 5230.2B
(b) NSHSBETHINST 5239.1B

1. **Purpose.** To establish an information management plan to determine and direct information management processes for Naval School of Health Sciences per references (a) and (b).
2. **Cancellation.** NSHSBETHINST 5230.1
3. **Background.** It is recognized that providing health care education is a complex endeavor that is highly dependent upon information management. Due to the collaborative nature of the command's mission, all activities performed must be coordinated and integrated throughout all departments and services. Because of the multi-disciplinary nature and interdependency of information, it is important that information resources be used effectively and efficiently.
4. **Mission.** To implement the information management plan at Naval School of Health Sciences in support of the following:
 - a. Providing customers with needed information in a timely manner.
 - b. Ensuring that careful attention is rendered to customer needs in building continuous access to a network of information.
 - c. Supporting the command mission and vision by providing timely access to a variety of data.
5. **Goal.** To obtain, manage and use information in improving individual and organizational performance, governance, management and administrative support.
6. **Scope and Direction.** To provide education, training and information in health care sciences, specialties, services

and management to enable uniformed services personnel to meet their mission in war and peace.

a. Human, hardware and software resources are used to supply information to support the organization's information management requirements. To meet these requirements, the directors have shared responsibility for the overall management of information.

b. The Executive Steering Council (ESC/Governing Body (GB)) has allocated financial resources to the management of information. Since information management is constantly changing and becoming more sophisticated, all additional needs for information management are assessed with appropriate financial considerations granted by the ESC/GB.

c. Major information systems are externally funded by the Assistant Secretary of Defense for Health Affairs (ASD/HA) or Naval Medical Information Management Center (NMIMC). The benefits of these systems, in addition to training, funding, guidance and support systems will be evaluated for application to the overall needs of this facility to ensure maximum educational support.

7. **Objectives.** Information management is a function, a set of processes and activities focused on meeting the command's information needs. Attention must be given to issues of timelines, accuracy, security, confidentiality, access, efficiency, collaboration, integrity and uniformity. Objectives specific to this command include:

a. Timely and easy access to complete information throughout the organization;

b. Improved data accuracy;

c. A demonstrated balance of proper levels of security versus access;

d. Use of aggregate data, along with external knowledge bases, comparative data and pursuing opportunities for improvement;

e. Redesign of important information-related processes to improve efficiency and greater collaboration and information sharing to effective training methodologies; and

f. Design of a multi-year plan to develop information resources and access.

8. **Assessing Information Management Needs.** Due to rapid changes and improvements in technology, a comprehensive assessment and reassessment of information management needs must be performed continuously. Needs assessment must be performed through review of the following categories:

- a. Setting or enhancement of services in providing training
- b. External and internal customer needs
- c. External regulatory needs
- d. Performance improvement needs assessment is based on review and analysis of command mission, goals, services, personnel, mode of service delivery, resources and access to affordable information technology. Following is a non-exhaustive list of areas to be considered in the assessment:
 - (1) Command's scope of services
 - (2) Internal and external customers served through information management
 - (3) Resources and support necessary for planning information and educational services
 - (4) Requirements for internal and external transmission of data and information
 - (5) Requirements for internally and externally generated data to support command-wide performance improvements
 - (6) Appropriateness of technologies utilized at the command
 - (7) Need to support customer/supplier relationships
 - (8) Enhancement of work flow activity
 - (9) Support needed for training and administrative decision-making
 - (10) Direction required for the scope and complexity of services provided
- e. Through assessment of information management needs, priorities will be developed for improving information management functions. Areas determined to have the greatest impact in

student training effectiveness will receive highest priority for process revision and enhancement.

f. Principles of information management will be discussed with the appropriate individuals during initial personnel orientation. Inservice training updates are provided on an "as needed" basis or during annual performance evaluation. Advanced principles are reviewed within each directorate as appropriate to their knowledge-base and complexity of information usage.

9. **Standards.** Timeliness and accuracy will be considered to ensure that security or confidentiality, access, efficiency and collaboration, integrity and uniformity of data are followed in overall information management functions.

a. Security and Confidentiality of Information.

(1) The command considers the need for appropriate levels of security and confidentiality of data and information.

(2) All policies and procedures will address the sensitive nature of student confidentiality and identify issues of release, retrieval and security of information.

(3) Individuals will have access to student data and information on a "need to know" basis, restricted to the level of authority, in accordance with command-wide policies and procedures governing information security and confidentiality.

(4) Physical infrastructure (cable plant) will follow the Department of Defense (DOD) and Military Health Services System (MHS) requirements for data standardization and open systems compliance guidelines.

b. Timeliness of information will have paramount importance in meeting the standards of the Command administrative policies and procedures.

c. Student Records. Student records are descriptions of training received. BUMED, Command, and accrediting organization regulations, policies, and procedures have set the required elements of the student's records.

d. External Database. Command provides information to external reference databases as required by law or when appropriate.

10. **Performance Improvement Information.** Appropriate information management will be required to allow appropriate

OCT - 6

design of processes for systematically measuring, assessing and improving performance. Performance improvement will be performed on a command-wide basis and will require integration of all information and data gathered throughout the facility.

11. **Strategic Considerations.** With continuous improvements in information management technology, considerations will include the following strategies:

- a. Application and implementation of programs
- b. Database communication and operating system strategy
- c. Hardware strategy
- d. Software strategy
- e. Organizational strategy
- f. Telecommunication strategy
- g. Future technology strategy

12. **Maintenance Services of Information Systems.** Maintenance services for systems not under warranty will be provided by the Management Information Systems Department (MIS) in conjunction with contracted maintenance services.

13. **Training.** Hands-on training will be provided for all information systems. Training for most major systems will be available at the command. Training on microcomputers will be provided locally through a commercial contract or at the Naval Computer and Telecommunications Station, Washington, D.C. The Management Information Systems Department will also make on-the-job training available on an emergency basis for standard office automation software packages. Command orientation will be used for introduction to onboard systems and computer security training.

14. **Contingency Planning and Operations.** Contingency Planning and Operations will be implemented as follows:

- a. Information systems within this command were engineered in such a manner that failure of connectivity in one section of the command will not affect the other wings or remote activity locations. All systems meet the Military Health Services System (MHS) data standardization and open systems requirements.

b. Back-up tapes for major information systems data will be stored in the main computer room with a secondary storage site determined by the Management Information System Department. Major information systems will be backed up on a nightly, weekly and monthly basis or as directed by the major claimant. Tapes must be rotated to ensure maximum recovery opportunities of the most recent data in case of total system failure.

c. Equipment and parts and supplies will be stocked to provide rapid recovery from failures.

d. Individual end-user microcomputers will be equipped with backup devices such as removable media (i.e. floppy disks or cartridges) or network storage areas for data back-up and recovery by end-users.

e. Uninterrupted Power Supplies or Underwriters Laboratories approved power strips must be used to protect equipment during power failures, spikes and brownouts.

15. **Computer Systems.** Computer systems within this command and subordinate activities include miscellaneous smaller information systems that operate on stand-alone personal computers (PCs) or on a local area network (LAN) that may include:

AWMSN- Automated Workload Management System Nursing
 BIOFACS - Biomedical and Facilities Equipment Systems
 CCDB - Central Credential Database
 CHCS - Composite Health Care System
 DRG E/G - Diagnosis Related Groups/Encoder/Grouper System
 EAS III - Expense Assignment System
 EIS - Executive Information System
 Internet Services - File Transfer Protocol, Worldwide Web,
 etc...
 MBTS - Medical Board Tracking System
 MED-OA - Medical Open Architecture
 MICRO-WORS Worldwide Outpatient Reporting System (CHCS
 version 4.4 will replace)
 MICRO-MICS - Microcomputer Medical Inventory Control System
 PMBS - Property Management and Budgeting System
 REGISTRAR - Academic Registration Grade and Transcription
 System
 SPMS - Standard Personnel Management System
 STARS-FL - Standard Accounting and Reporting System-Field
 Level
 TMED - Telemedicine/Telemanagement System
 TOPS - Three Year Obligation Performance System
 TPOCS - Third Party Outpatient Collection System
 COTS - Commercial Off-The-Shelf Programs

OCT - 6

Various CD-ROM Subscription database (i.e., MSDS, Medline, etc.)

VTC - Video Teleconferencing System

16. **Information System Executive Board (ISEB)**. The ISEB is a standing committee which formulates local policy, consistent with Department of Navy and Department of Defense policy, recommends approval action for new systems and establishes priorities for development of local systems. ISEB is responsible for implementation of the Information Management Plan. The committee will meet quarterly or more frequently if required by the Chairman. Board members are appointed by the Commanding Officer.

17. **Information Systems Acquisitions**. Systems acquisitions follow a life cycle management approach. The documentation and approval for information systems projects vary depending upon cost and complexity of the project. BUMED policy is to develop ways to simplify and streamline the acquisition process so that small computer systems and automated data processing services can be acquired rapidly and put to effective use. Reference (a) outlines the process for acquisition of new or replacement systems.

18. **Life Cycle Management**. Documentation associated with the acquisition, modification or expansion of information technology resources must be retained throughout the system life cycle.

19. **System Change Requests**. Recommended system change requests for major DOD/DON systems may be submitted by any system user. The change request will be evaluated by the MIS Dept. Minor changes, such as report format changes that are feasible for MIS Dept. to perform will be scheduled for completion. This process will be in coordination with the department head or the director of the requester to ensure changes made are appropriate. Major changes that are beyond capabilities or scope of responsibilities of MIS Dept. will be submitted through the chain of command to the appropriate Configuration Control Board.

20. **System Incident Reports**. System incident reporting for major DOD/DON systems may be submitted by any user. System incident reports will be reviewed by the MIS department for validity. Valid system incident reports will be forwarded to the appropriate Configuration Control Board for action. Any system incident report determined to be a threat to personnel safety is automatically classified as high criticality and a quick fix is generated and applied to resolve the problem.

21. **Electronic Mail (e-mail)**. E-mail is a tool that can aid the smooth, efficient and timely conduct of business. E-mail accounts allow information to be informally sent and received at the convenience of the person using the resource. E-mail allows for quick query and reporting of time sensitive information between activities. E-mail is an adjunct to traditional methods, but does not replace official correspondence practices.

a. Definitions

(1) Authorized user. A department or person authorized to directly utilize electronic mail using federally-owned resources.

(2) E-Mail Station. Any government owned computer system used for receipt or transmission of electronic mail.

(3) Internal E-mail. Access is provided to the mailman module of NMMC's CHCS module. The current CHCS configuration does not allow transmission or receipt of electronic mail beyond the individual command end-users and subordinate activities.

(4) External E-mail. Current BUMED policy authorizes the use of a variety of freeware and commercial versions of mail reader programs that are Post Office Protocol and Simple Mail Transfer Protocol compliant. Programs will be operated by connecting to the command mail server system. External e-mail is used for internet e-mail worldwide.

b. Responsibilities

(1) MIS department will be responsible for periodic monitoring, controlling, and coordination of e-mail utilization and will provide periodic training to authorized users. The ISEB meeting will be the forum to address major e-mail related issues.

(2) Department Heads will exercise control over electronic mail stations in their area and ensure that e-mail is being used properly. They will monitor usage and coordinate with the MIS Department in verifying compliance with the established procedures.

c. Sending E-mail

(1) Authorized users will not send e-mail outside the command addressing policy issues unless each individual message is approved by the Commanding Officer prior to release. Authorized users will transmit a copy of all outgoing

policy-related e-mail to the Commanding Officer, along with a carbon copy to the Director for Administration.

(2) Use of e-mail for proprietary purposes, sending or receiving messages which are not in compliance with Navy Equal Opportunity Program Standards, or use for illegal activities is strictly prohibited.

d. Receiving E-mail

(1) All incoming official e-mail taskings received via electronic mail will be forwarded to the Administrative Support Department to be processed and distributed in accordance with local correspondence handling and routing procedures.

(2) Due to mail server storage limitations, all individuals with assigned accounts will check their e-mail account regularly for incoming messages.


D. A. WYNKOOP

Distribution:
List I and II